

Electronic Monitoring and Surveillance

Policy Statement

NorthStar Regional recognizes the need to strike a balance between an individual's right to be free from invasion of privacy and the organization's duty to promote a safe environment for all residents, client's, employees, and visitors. Surveillance cameras may be installed in places where security of either property or people would likely need to be enhanced. NorthStar Regional abides by all federal and state patient privacy rights laws, including HIPAA.

Procedures

1. The purpose of NorthStar Regional-owned and managed video camera surveillance systems is to:
 - a) Promote a safe environment by deterring acts of harassment or assault.
 - b) Deter theft and vandalism and assist in the identification of individuals who commit damage to NorthStar Regional property.
 - c) Assist law enforcement agencies with regard to the investigation of any crime that may be captured.
 - d) Assist in the daily operations of the organization.
2. Upon admission to the facility, clients and new staff will be informed of NorthStar Regional's use of video camera's and recording in common areas. Clients will be informed that recordings will not be released under any circumstances to anyone outside of NorthStar regional unless a valid court order is secured and verified. Clients will be asked to sign an acknowledgment they have been informed of this.
3. Signs will be posted in appropriate areas, either at the entrance to the area under surveillance or in close proximity to the camera, informing the general public of the usage of video surveillance on the premises.
4. The Chief Operating Officer will be consulted prior to adding or moving surveillance cameras to other areas. The Chief Operating Officer, Chief Executive Officer, Residential Program Directors and/or Chief Compliance Officer are the only staff members authorized to determine the location and placement of a surveillance camera.
5. Only designated personnel (Program Directors and/or Senior Leadership) will have access to the monitors or to the recordings made in the course of the surveillance. Personal information contained on the recordings shall not be used or disclosed for purposes other than those for which it was collected, except with the written consent of the individual or as required or mandated by law or court order.
6. Surveillance cameras will not be placed in areas where there is a reasonable expectation of privacy by an individual (i.e., bathrooms, resident rooms, procedure rooms, etc.).
7. Cameras and electronic monitoring equipment set up for sending and storing of video recordings will be accessed by a limited number of staff who have been pre-approved by the Chief Operation Officer and/or Chief Executive Officer. Monitoring activities will always be conducted according to the "minimum necessary" standard of HIPAA. Individual staff members are expected to adhere to securing viewing devices by utilizing a password, passcode, two-factor authentication, and to follow policy 4.0.0 in the NorthStar Regional HIPAA Manual, Mobile Device Management Protocol and Guidelines.
8. Prior to the initial or expansion of any video monitoring system the Chief Operations Officer, Chief Executive Officer, and/or Chief Compliance Officer shall approve the technology and verify requirements

needed for any equipment prior to purchase or install.

9. Information obtained from the cameras will be used exclusively for law and/or internal policy enforcement, except with the consent of the individual or as required by court order.

10. All camera installations and use are subject to federal and state laws.

11. To satisfy each resident's expectation of privacy in his or her own room, NorthStar Regional does not permit any electronic monitoring, covert or otherwise, of residents in their own rooms.

12. NorthStar Regional will remove any device capable of electronic monitoring from a resident's room if discovered by or reported to our staff.

13. In addition, NorthStar Regional has the right, in its sole discretion, to request that any recording obtained through unauthorized electronic monitoring as prohibited by NorthStar Regional's policies be destroyed in the presence of a representative of NorthStar Regional's administration. If NorthStar Regional discovers that this policy has been violated, the resident violating the policy (or the resident's legal representative) shall be responsible for any costs to remove any such electronic monitoring and for any costs associated with any claims, damages, or injuries arising as a result of the violation of this policy.

14. Electronic monitoring includes visual and audio recordings of individuals by means of any device, recording system, video surveillance camera, web-based camera, or videophones (including but not limited to cellular phones or smartphones), regardless of whether these are interactive or simply recording devices.

15. NorthStar Regional will abide by Minnesota Statutes 626A.01 and 626A.02, as well as Federal wiretapping laws by not releasing any recording to any unauthorized person except as compelled by Court Order.